

Abstract of the Disclosure

A logic circuit for performing modular multiplication of a first multi-bit binary number and a second multi-bit binary number is provided. Combination logic combines the second multi-bit binary value with a group of W bits of the first multi-bit binary value every j^{th} input cycle to generate W multi-bit binary combination values every j^{th} input cycle, where the W bits comprise bits jW to $(jW + W - 1)$, $W > 1$, j is the cycle index from 0 to $k - 1$, $k = N/W$, and N is the number of bits of the first multi-bit binary value. Thus in this way a plurality of multi-bit binary combinations are input every cycle in a parallel manner. Accumulation logic holds a plurality of multi-bit binary values accumulated over previous cycles. Reduction logic generates a W bit value Λ in a current cycle for use in the next cycle. A multi-bit modulus binary value is received and combined with the W bit value Λ generated in a current cycle to generate W multi-bit binary values for use in the next cycle. Combination logic receives the combinations from the combination logic and the W multi-bit binary values from the reduction logic as well as the binary values held by the accumulator logic to generate new multi-bit binary values for input to the accumulator logic to be held for the next cycle. The reduction logic generates the W bit value Λ based on the multi-bit modulus binary value, the multi-bit binary values held in the accumulator logic, W multi-bit binary combination values generated by the combination of the second multi-bit binary value and a group of W bits of the first multi-bit binary value in the current cycle, and the W bit value Λ generated for the current cycle.

"Express Mail" mailing label number: EL873858905US

Date of Deposit: December 20, 2001

This paper or fee is being deposited on the date indicated above with the United States Postal Service pursuant to 37 CFR 1.10, and is addressed to the Commissioner for Patents, Box Patent Application, Washington, D.C. 20231.

10027237 423001